

FSA Integration Partner Program
United States Department of Education
Office of Federal Student Aid



**Security Architecture Status Report –
August – September 2003**

Deliverable #120.2.3

***Task Order #120:
Security and Privacy Support***

Version 1.0

September 30, 2003

Document Revision History

Version Number	Date	Author	Revisions Made
1.0	September 30, 2003	Jesse Bowen	Initial submission

Table of Contents

1	Executive Summary	4
2	Introduction.....	5
3	Security Architecture Status Overview.....	6
3.1	Background	6
3.2	Task Order Objectives	6
3.3	Progress to Date	7
3.4	Next Steps	7
4	Security Architecture Communications Plan Status	9
4.1	Introduction.....	9
4.2	Goals of the Security Architecture Communications Plan	9
4.3	Communication Opportunities.....	9
5	IT Security and Privacy Policy Gap Analysis.....	10
5.1	Introduction.....	10
5.2	Gap Analysis Matrix	10
6	Status of Certification and Accreditation Support	14
6.1	CDDTS Security Risk Assessment.....	14
6.2	Support for Tier 2 Certification and Accreditation Activities	16
7	Appendix.....	17
7.1	Management Council Update on Enrollment and Access Management	17
7.2	Security Architecture Briefing for FSA System Security Officers.....	17
7.3	Enrollment and Access Management Core Team Meeting	17
7.4	Evaluation of CDDTS Corrective Action Plan.....	17

1 Executive Summary

This document constitutes a required interim deliverable for Federal Student Aid Task Order 120 – Security and Privacy Support.

A new Task Area, 3.12, was recently added to TO 120 to cover security architecture support activities. The security architecture support will include specific tasks as well as *ad hoc* support for security architecture and integration questions. It will also cover integration issues and activities arising from other FSA projects.

This report summarizes activities performed in support of the FSA Security and Privacy Architecture during August and September of 2003. This report consists of the following major sections:

Section 3 – Security Architecture Status Overview provides an introduction to the work in progress, and summarizes the status of current activities being conducted in support of the FSA Security and Privacy Architecture.

Section 4 – Security Architecture Communications Plan Status summarizes the meetings and other opportunities used to promote the FSA Security and Privacy Architecture with internal and external groups.

Section 5 – IT Security and Privacy Policy Gap Analysis summarizes areas in the FSA IT Security and Privacy Policy that may need to be updated or added to support the FSA Security and Privacy Architecture.

Section 6 – Certification and Accreditation Support Status provides an overview of the activities related to follow-up from the CDDTS Security Risk Assessment, and to support Tier 2 systems.

Section 7 – Appendix contains supplemental presentations and reports related to Security and Privacy Architecture:

- Management Council Update on Enrollment and Access Management
- Security Architecture Briefing for FSA System Security Officers
- Enrollment and Access Management Core Team Meeting
- Evaluation of CDDTS Corrective Action Plan

2 Introduction

This document is a required deliverable for Task Order 120 – Security and Architecture Support. TO 120 provides support to FSA for a variety of security and privacy support activities. A recent modification to the task order added activities related to security architecture to TO 120. This document is a status report on the activities conducted during August and September of 2003, are that are in progress, related to support of development and deployment of the FSA Security and Privacy Architecture.

This deliverable contains the following major sections:

- Security Architecture Status Overview (Section 3)
- Security Architecture Communications Plan Status (Section 4)
- IT Security and Privacy Policy Gap Analysis (Section 5)
- Certification and Accreditation Support Status (Section 6)
- Appendix (Section 7), consisting of:
 - Management Council Update on Enrollment and Access Management
 - Security Architecture Briefing for FSA System Security Officers
 - Enrollment and Access Management Core Team Meeting
 - Evaluation of CDDTS Corrective Action Plan

3 Security Architecture Status Overview

3.1 Background

FSA recently completed a project under Task Order 124 to create a Security and Privacy Architecture Framework, Specification, and Implementation Strategy. The implementation strategy recommended several actions that will prepare FSA for development and deployment of security standards and services, and will promote understanding and adoption of the FSA Security and Privacy Architecture.

FSA defined several tasks that will support follow-on activities related to continued development of security architecture components. FSA created an SOO to define this work, and submitted it to the Integration Partner Program on June 23, 2003. The Security Architecture support activities will be organized as a modification to Task Order 120 – Security and Privacy Support. A modified Technical Proposal for Task Order 120 was submitted by the Integration Partner Program on July 7, 2003. FSA accepted the modified Technical Proposal, and subsequently awarded a modification to Task Order 120 to cover the security architecture support objectives and deliverables.

3.2 Task Order Objectives

A new Task Area, 3.12, was added to TO 120 to cover security architecture support activities. This task area will provide half-time staffing of a Senior Security Architect to act as a security Subject Matter Expert. The security architect will also aid the FSA security organization with planning and delivering initial components of the security architecture. The security architecture support will include specific tasks as well as *ad hoc* support for security architecture and integration questions. It will also cover integration issues and activities arising from other FSA projects (such as Data Strategy and PIN Reengineering Analysis) that have security architecture implications.

The specific objectives of Task Area 3.12 are:

1. Begin preparation work for developing the FSA security architecture
 - Assist FSA with communicating the Security Architecture vision to CIO and business groups
 - Perform a gap analysis of the existing FSA IT Security and Privacy Policy to define policies and standards that will require modification or development to support the FSA Security Architecture
 - Create recommended web security guidelines
 - Recommend data classification definitions for classifying the sensitivity of FSA data
 - Provide general security architecture support, such as attending *ad hoc* meetings and advising FSA as a security subject matter expert
2. Support system risk assessments and Certification & Accreditation activities
 - Assist preparation of up to four Tier 2 systems for Certification & Accreditation
 - Tier 2 systems in scope may include PGA, LMS, IFAP, and eCB
 - Assess any additional information needed to prepare for C&A
 - Work with SSOs for the systems to prepare C&A documentation
 - Support risk assessment of the Disability Discharge Tracking System (CDDTS)

3.3 *Progress to Date*

Activities in support of the FSA Security and Privacy Architecture are described below and in greater detail in Sections 4 – 6.

The FSA Security and Privacy Architecture has been communicated to a variety of audiences, including the Business Integration Group, the FSA Management Council, and the FSA System Security Officers. Meetings are also planned to discuss the FSA Security and Privacy Architecture Framework with the FSA CIO Technical Architecture group and with the Department of Education.

The Enrollment and Access Management project is developing recommendations and a high-level design to address FSA needs for managing trading partner registration and access privileges. Coordination with the Enrollment and Access Management team is helping insure that solution options and recommendations arising from this work will be consistent with the intent of the FSA Security and Privacy Framework. Deliverables currently being developed are summarized in the following section and in the Appendix.

Analysis of the existing IT Security and Privacy Policy was performed to identify policy areas that will need to be modified or added to support the FSA Security and Privacy Architecture. Eighteen major items were identified. These potential gaps are documented in greater detail in Section 5.

Support for FSA Certification and Accreditation activities are described in Section 6, below. The Corrective Action Plan prepared in response to the CDDTS Security Risk Assessment was evaluated, and the analysis is attached in the Appendix. Assistance was also provided to the IFAP SSO to review proposed approaches for the CAP being developed for that system.

Weekly status meetings continue with the FSA Chief Security Officer. These status meetings review work in progress, provide an opportunity for planning upcoming activities, and provide an opportunity for communicating progress on other task orders that will affect the FSA Security and Privacy Architecture.

3.4 *Next Steps*

Major areas of work over the next reporting period for this task order are:

- **Develop web security standards:** Web security standards will be developed as outlined in the Gap Analysis Matrix presented in Section 5.
- **Develop a data classification structure:** Draft recommendations for Data Classification Definitions will be created to define data classification levels and next steps for implementing a data classification process.
- **Prepare a Final Report on Security Architecture Support Activities:** This report will summarize actions completed during the course of this task order in support of implementing the FSA Security Architecture.
- **Implement Communications Plan:** Continue communications with internal and external groups to explain and promote the FSA Security and Privacy Architecture.

- **Coordinate with Other FSA Initiatives:** Continue coordination activities with teams working on related task orders, including:
 - Enrollment and Access Management team
 - Technical Strategies team
 - PIN Reengineering team
 - The recently awarded Identity and Access Management Tools Analysis team.

4 Security Architecture Communications Plan Status

4.1 Introduction

A draft Communication Plans was developed as part of the initial status report for this task order¹. The goal of the communications plan was to define the major messages and audiences that should be approached to better educate various FSA constituencies on the goals, benefits, and plans for implementation of the FSA Security and Privacy Architecture. This section summarizes specific opportunities that have been used to provide information to FSA business organizations and projects. For reference, several presentations used in these meetings are included in the Appendix to this report.

4.2 Goals of the Security Architecture Communications Plan

The major goals of the security architecture communications plan are to:

- Identify the primary and secondary internal and external audiences for messages about the FSA security architecture.
- Promote integration of the FSA security architecture into FSA business planning and development of new capabilities.
- Convey the major security architecture principles that form the basis for development and operation of the FSA security architecture.
- Provide opportunities to solicit feedback from system owners as a means of enhancing understanding and acceptance of the FSA security architecture.
- Develop effective communications vehicles for continued development and improvement of FSA security architecture services.

4.3 Communication Opportunities

Communications about the FSA security architecture vision were part of the following meetings during August and September:

- FSA Management Council Meeting (8/25/2003, presentation attached)
- FSA System Security Officer Meeting (8/26/2003, presentation attached)
- Enrollment and Access Management Core Team Meeting (9/4/2003, presentation attached)
- Business Integration Group Meeting (9/9/2003)

In addition, the FSA Security and Privacy Architecture has been addressed during several meetings with the Technical Strategies Core Team on web services and web usage.

Meetings with the FSA CIO Architecture Working Group and Department of Education technical architecture representatives are being planned.

¹ Deliverable 120.2.1 -- Security Architecture Status Report – June-July 2003, July 31, 2003
Confidential – For Official Use Only

5 IT Security and Privacy Policy Gap Analysis

5.1 Introduction

The FSA IT Security and Privacy Policy establishes overall guidance for protecting FSA systems and data. The policy defines three major areas of controls: Enterprise Management Controls, Operational Controls, and Technical Controls. Although the policy provides high-level vision and expectations, it does not specify detailed standards or procedures for all areas of interest to FSA security and privacy objectives.

One of the recommendations from the FSA Security and Privacy Architecture Framework project² was that security technical architecture standards should be developed to support implementation of the FSA Security and Privacy Architecture. This section identifies gaps in the existing IT Security and Privacy Policy that should be addressed to provide a more complete set of technical standards for that purpose. Gaps are identified and classified as to type. Recommendations are then provided that summarize the major issues to be addressed to achieve a comprehensive structure of security and privacy policies, standards, and guidelines.

5.2 Gap Analysis Matrix

The table below describes the policy areas in the FSA IT Security and Privacy Policy that may need additional development to support deployment of the FSA Security and Privacy Architecture. Each potential gap is identified with the associated policy area, the specific section or sections affected, nature of the gap, and recommendations for addressing the gap.

Policy Area	Section(s)	Gap No.	Gap	Recommendation
Enterprise Management Controls	Introduction	1	The introduction to the Enterprise Management Controls section does not reference the FSA Security and Privacy Architecture or management requirements for architecture components	<ul style="list-style-type: none"> • Insert reference to FSA Security and Privacy Architecture • Insert discussion of how management controls relate to FSA Security and Privacy Architecture • Insert new section under Enterprise Management that describes review and update requirements for FSA Security and Privacy Architecture • Insert section under Enterprise Management that describes processes for integrating FSA Security and Privacy Architecture with the FSA IT Technical Architecture • Insert section under Enterprise Management that describes processes for integrating FSA

² Task Order 124: Security and Privacy Architecture Framework, Deliverable 124.1.2 – Final Security and Privacy Architecture Report, May 30, 2003
Confidential – For Official Use Only

Policy Area	Section(s)	Gap No.	Gap	Recommendation
				Security and Privacy Architecture with the Department of Education IT Technical Architecture and Security Architecture
Enterprise Management Controls	2.1 Risk Management	2	The Risk Management process and requirements do not reference the FSA Security and Privacy Architecture	<ul style="list-style-type: none"> • Insert reference to FSA Security and Privacy Architecture • Insert requirement that risk assessments address risks associated with not using existing Security and Privacy Architecture components, or of deviating from architecture standards.
Enterprise Management Controls	2.2 Security Control Reviews	3	References FSA IT Architecture but not FSA Security and Privacy Architecture	<ul style="list-style-type: none"> • Insert reference to FSA Security and Privacy Architecture • Insert requirement that new security controls be consistent with Security and Privacy Architecture
Enterprise Management Controls	2.3 System Security Plan	4	Does not require the System Security Plan to describe integration with FSA Security and Privacy Architecture	<ul style="list-style-type: none"> • Require the System Security Plan to describe how system security controls interact with the FSA Security and Privacy Architecture
Enterprise Management Controls	2.5 Solution Life Cycle	5	FSA Security and Privacy Architecture is not referenced in the FSA Solution Life Cycle (SLC) or Security Process Guide	<ul style="list-style-type: none"> • Refer to the FSA Security and Privacy Architecture in the FSA SLC and Security Process Guide • Require that existing FSA Security and Privacy Architecture components and standards be used if possible in new solutions
Enterprise Management Controls	2.8 System Interconnections	6	Existing requirements for Memoranda of Understanding (MOU) and/or Memoranda of Agreement (MOA) do not discuss interactions with security components, functions, or standards that will be part of the FSA Security and Privacy Architecture	Insert discussion of how FSA Security and Privacy Architecture components may involve system interconnections that may require MOU or MOA.
Operational Controls	3.1 Personnel Security	7	User administration processes described in this section do not reference the FSA Security and Privacy Architecture components that will enable these processes	<ul style="list-style-type: none"> • Insert discussion of how FSA Security and Privacy Architecture components and standards will affect these processes • As components and standards for the FSA Security and Privacy Architecture are implemented, create detailed standards and procedures for user administration tasks

Policy Area	Section(s)	Gap No.	Gap	Recommendation
Operational Controls	3.1.3 Sensitivity/Risk Levels	8	There are no FSA definitions of data classification levels or security sensitivity levels	<ul style="list-style-type: none"> • Include security level definitions (e.g., NIST Security Classifications) for FSA systems • Develop data classification definitions for FSA data
Operational Controls	3.1.5 Use of External Connections	9	Section does not reference use of external connections by trading partners	Insert requirements for external trading partners that use FSA systems
Operational Controls	3.1.6 Nondisclosure and Confidentiality Agreements	10	Section discusses FSA employees and contractors, but not requirements for FSA trading partners that use FSA systems	Insert requirements for nondisclosure agreements and confidentiality agreements for FSA trading partners.
Operational Controls	3.3 Production Input/Output Controls	11	Section does not discuss data input and output through web applications (e.g., by trading partners)	<ul style="list-style-type: none"> • Insert requirements for data input and output in web applications • Insert requirements for data input and output by trading partners
Technical Controls	Introduction	12	No requirement to consider use of FSA Security and Privacy Architecture components when developing technical security controls	Include discussion of FSA Security and Privacy Architecture and how it should be used when developing or reviewing technical security controls for FSA systems.
Technical Controls	All	13	There are no detailed standards defined as part of the FSA security and privacy policy structure for specific types of technical controls, as identified in the items below	<ul style="list-style-type: none"> • Modify the structure of the FSA IT Security and Privacy Policy to include a section for technical standards • Create specific technical standards, as discussed in the items below
Technical Controls	All	14	No technical standards for web security	<p>Develop web security standards that define:</p> <ul style="list-style-type: none"> • Scope and applicability of standard • Integration of web security standards into FSA SLC • Security web servers and hosts • Web application security <ul style="list-style-type: none"> ○ coding standards and practices ○ web application design principles ○ web application security tools ○ web application testing • Use of web services security standards • Encryption standards for web applications • Infrastructure design for web applications

Policy Area	Section(s)	Gap No.	Gap	Recommendation
				<ul style="list-style-type: none"> • Hosting provider requirements for web components
Technical Controls	All	15	No technical standards for electronic signatures	Define standards for electronic signatures
Technical Controls	All	16	No technical standards for encryption	Define standards for encryption
Technical Controls	All	17	No technical standards for network and infrastructure security	Define technical standards for network and infrastructure components: <ul style="list-style-type: none"> • Firewalls • VPNs • Intrusion detection and prevention systems • Security monitoring systems
Technical Controls	All	18	No technical standards or security SLA requirements for outsourced and contractor-provided security services	<ul style="list-style-type: none"> • Develop security standards and security SLA requirements to include in contracts for externally hosted systems and data centers • Develop an interim strategy to address security requirements for existing contracts

6 Status of Certification and Accreditation Support

The security architecture support activities added to the modified TO 120 – Security and Privacy Support include assistance with FSA Certification and Accreditation efforts in two major areas:

- Assistance with Certification and Accreditation for FSA Tier 2 systems
- Performing a security assessment on CDDTS.

6.1 CDDTS Security Risk Assessment

The CDDTS Security Risk Assessment was conducted during July and August. The final report was submitted on August 15³. Subsequently, ACS, the CDDTS contractor, prepared a Corrective Action Plan (CAP) that provided responses to the findings in the risk assessment. Appendix 7.4 contains a report that evaluates the responses in the corrective action plan. Some of the findings were addressed by additional information provided by the contractor. Other findings are in the process of being remediated and will need to be reevaluated after corrective actions or improvements have been completed.

The table below summarizes the actions proposed in the CAP, an evaluation of how they address the risk assessment findings, and their current status.

Summary of status for corrective actions proposed for CDDTS in response to the risk assessment conducted in August 2003.

Observation Number	Observation Summary	Status of Corrective Action	Expected Completion Date
M1	Security testing of changes is not part of the CDDTS configuration management plan.	In progress	Not supplied
M2	Anti-virus tools are not run on the CDDTS server.	Closed	--
M3	Security training during employee orientation is brief and not documented.	In progress	9/30/2003
M4	Disaster recovery plans have not been tested.	Planned	9/19/2003
M5	Business continuity plans have not been tested.	Planned	9/19/2003
M6	A security training and awareness program has not been fully implemented.	In progress	9/30/2003
M7	Several critical security services are performed for CDDTS by contractor divisions that may be acquired by a	Pending (FSA should continue to monitor the status of	--

³ Deliverable 120.2.2 -- Security Risk Assessment for Conditional Disability Discharge Tracking System (CDDTS), August 15, 2003

Observation Number	Observation Summary	Status of Corrective Action	Expected Completion Date
	third party.	security services provided by third parties)	
M8	Security risk analysis and testing is not included in the configuration management plan.	In progress	10/10/2003
M9	Off-site storage of back-up media and business continuity locations are relatively close to the primary CDDTS Data Center.	Closed	--
O1	Authorized access is not reviewed annually.	Closed	--
T1	Audit trail logging and review are not routinely performed.	In progress	9/19/2003
T2	User passwords for the CDDTS application are stored in clear text.	In progress	9/19/2003
T3	There are no functions to detect and lock accounts after repeated login failure.	In progress	9/19/2003
T4	The System Security Plan does not specify periodic scanning for unauthorized modems.	In progress	9/19/2003
T5	An Intrusion Detection System is not yet fully implemented.	In progress	9/19/2003
T6	Firewall policies and filtering rules should be audited.	Closed	--
T7	CDDTS accounts are not configured for automatic logout after periods of inactivity.	Pending (System Security Plan should be updated)	--
T8	Some file transfers to CDDTS are made through standard FTP.	Pending (System Security Plan should be updated)	--
A1	No CDDTS asset inventory.	Closed	--
A2	A FISMA Privacy Impact Assessment has not been performed.	Pending (A privacy impact assessment should be conducted according to recently published FSA guidelines)	--
A3	The System Security Plan is missing some required content.	In progress	10/10/2003

6.2 Support for Tier 2 Certification and Accreditation Activities

Two FSA systems identified as Tier 2 are undergoing Certification and Accreditation: Student Portal and IFAP. Teams for both systems were contacted to determine if assistance with C&A activities were required.

The Student's Portal team responded that C&A activities were nearly complete, and that no additional assistance was required. The Student's Portal production system went live on September 7, 2003.

Lloyd Nicholson requested support to review the Corrective Action Plan being prepared for IFAP. At a meeting on September 5, 2003, each item to be addressed by the IFAP CAP was reviewed. Additional suggestions and strategies for defining and explaining the corrective actions were provided. Additional review and support for development of the IFAP CAP will be provided as required.

7 Appendix

The appendix materials for this status report consist of the following supplementary information.

7.1 Management Council Update on Enrollment and Access Management

(Presentation conducted August 25, 2003)

7.2 Security Architecture Briefing for FSA System Security Officers

(Presentation conducted August 26, 2003)

7.3 Enrollment and Access Management Core Team Meeting

(Presentation conducted September 4, 2003)

7.4 Evaluation of CDDTS Corrective Action Plan

(Evaluation of Corrective Action Plan submitted in response to the CDDTS Security Risk Assessment⁴)

⁴ Deliverable 120.2.2 -- Security Risk Assessment for Conditional Disability Discharge Tracking System (CDDTS), August 15, 2003